Department of Homeland Security
Office of Inspector General

Information Technology Management Letter for the FY 2008 Transportation Security Administration Financial Statement Audit (Redacted)

Notice: The Department of Homeland Security, Office of Inspector General has redacted the report for public release. A review under the Freedom of Information Act will be conducted upon request.

OIG-09-62

April 2009

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 23, 2009

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report presents the information technology (IT) management letter for the FY 2008 Transportation Security Administration (TSA) financial statement audit as of September 30, 2008. It contains observations and recommendations related to information technology internal control that were not required to be reported in the financial statement audit report (OIG-09-09, November 2008) and represents the separate restricted distribution report mentioned in that report. The independent accounting firm KPMG LLP (KPMG) performed the audit of TSA's FY 2008 balance sheet and prepared this IT management letter. KPMG is responsible for the attached IT management letter dated March 6, 2009, and the conclusions expressed in it. We do not express opinions on TSA's financial statements or internal control or make conclusions on compliance with laws and regulations.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

KPMG LLP
2001 M Street, NW
Washington, DC 20036

March 6, 2009

Inspector General
U.S. Department of Homeland Security

Chief Information Officer
Transportation Security Administration

Chief Financial Officer
Transportation Security Administration

Ladies and Gentlemen:

We audited the consolidated balance sheet of the U.S. Department of Homeland Security (DHS) Transportation Security Administration (TSA) as of September 30, 2008. The objective of our engagement was to express an opinion on the fair presentation of the consolidated balance sheet of TSA. In connection with our fiscal year 2008 audit, we also considered TSA's internal controls over financial reporting, and tested TSA's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on the consolidated balance sheet of TSA.

In connection with our fiscal year (FY) 2008 engagement, we considered TSA's internal control over financial reporting by obtaining an understanding of TSA's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our procedures. We limited our internal control testing to those controls necessary to achieve the objectives described in *Government Auditing Standards* and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements*. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982* (FMFIA). The objective of our engagement was not to provide an opinion on the effectiveness of TSA's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of TSA's internal control over financial reporting. Further, other matters involving internal control over financial reporting may have been identified and reported had we been able to perform all procedures necessary to express an opinion on the TSA balance sheet as of September 30, 2008, and had we been engaged to audit the other FY 2008 financial statements.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects TSA's ability to initiate, authorize, record, process, or report financial data reliably in accordance with U.S. generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of TSA's financial statements that is more than inconsequential will not be prevented or detected by TSA's internal control over financial reporting. A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control.

KPMG

During our audit engagement, we noted certain matters with respect to TSA's financial systems' information technology (IT) general controls which we believe contribute to a TSA-level significant deficiency that is considered a material weakness in IT general and application controls. These matters are described in the *IT General Control Findings by Audit Area* section of this letter.

The material weakness and significant deficiency described above are presented in our *Independent Auditors' Report*, dated March 6, 2009. This letter represents the separate restricted distribution report mentioned in that report.

Although not considered to be material weaknesses, we also noted certain other matters during our audit engagement which we would like to bring to your attention. These matters are also described in the *IT General Control Findings by Audit Area* section of this letter.

The material weakness and other comments described herein have been discussed with the appropriate members of management, or communicated through a Notice of Finding and Recommendation (NFR), and is intended **For Official Use Only**. We aim to use our knowledge of TSA's organization gained during our audit engagement to make comments and suggestions that we hope will be useful to you. We have not considered internal control since the date of our *Independent Auditors' Report*.

The Table of Contents on the next page identifies each section of the letter. In addition, we have provided: a description of key TSA financial systems and information technology infrastructure within the scope of the FY 2008 TSA balance sheet audit in Appendix A; a description of each internal control finding in Appendix B; and the current year status of the prior year NFRs in Appendix C. Our comments related to financial management and reporting internal controls have been presented in a separate letter to the Office of Inspector General and the TSA Chief Financial Officer dated March 6, 2009.

This report is intended solely for the information and use of TSA and DHS management, DHS Office of Inspector General, OMB, U.S. Government Accountability Office, and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

INFORMATION TECHNOLOGY MANAGEMENT LETTER

TABLE OF CONTENTS

APPENDICES

OBJECTIVE, SCOPE AND APPROACH

We were engaged to perform an audit of the Transportation Security Administration's (TSA) Information Technology (IT) general controls in support of the fiscal year (FY) 2008 TSA balance sheet audit engagement. The overall objective of our engagement was to evaluate the effectiveness of IT general controls of TSA's financial processing environment and related IT infrastructure as necessary to support the engagement. The U.S. Coast Guard's hosts key financial applications for TSA. As such, our audit procedures over information technology (IT) general controls for TSA included testing of the Coast Guard's policies, procedures, and practices, as well as at TSA Headquarters.

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the Government Accountability Office (GAO), formed the basis of our audit. The scope of the TSA IT general controls assessment is described in Appendix A. FISCAM was designed to inform financial auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial audit. FISCAM also provides guidance to IT auditors when considering the scope and extent of review that generally should be performed when evaluating general controls and the IT environment of a federal agency. FISCAM defines the following six control functions to be essential to the effective operation of the general IT controls environment.

- *Entity-wide security program planning and management (EWS)* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
- *Access control (AC)* – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.
- *Application software development and change control (ASDCC)* – Controls that help to prevent the implementation of unauthorized programs or modifications to existing programs.
- *System software (SS)* – Controls that limit and monitor access to powerful programs that operate computer hardware and secure applications supported by the system.
- *Segregation of duties (SD)* – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- *Service continuity (SC)* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

To complement our general IT controls audit, we also performed technical security testing for key network and system devices, as well as testing over key financial application controls. The technical security testing was performed both over the Internet and from within select Coast Guard and TSA facilities, and focused on test, development, and production devices that directly support TSA's financial processing and key general support systems.

In addition to testing TSA's general control environment, we performed application control tests on a limited number of TSA's financial systems and applications. The application control testing was performed to assess the controls that support the financial systems' internal controls over the input, processing, and output of financial data and transactions.

- *Application Controls (APC)* - Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

During fiscal year (FY) 2008, TSA took corrective action to address prior year IT control weaknesses. For example, TSA made improvements in testing disaster recovery procedures, reviewing audit logs, and implementing emergency response training for all personnel with data center access. However, during FY 2008, we continued to identify IT general control weaknesses that impact TSA's financial data. The most significant weaknesses from a financial statement audit perspective related to controls over the termination of the contract with the software support vendor, the design and implementation of configuration management policies and procedures, and the development, implementation, and tracking of scripts at Coast Guard's . Collectively, the IT control weaknesses limited TSA's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, these weaknesses negatively impacted the internal controls over TSA financial reporting and its operation and we consider them to collectively represent a material weakness for TSA under standards established by the American Institute of Certified Public Accountants (AICPA). In addition, based upon the results of our test work, we noted that TSA did not fully comply with the requirements of the *Federal Financial Management Improvement Act* (FFMIA).

Of the 15 findings identified during our FY 2008 testing, 13 are repeated findings, either partially or in whole from the prior year, and 2 are new IT findings. These findings represent weaknesses in four of the six FISCAM key control areas. Specifically, 1) unverified access controls through the lack of comprehensive user access privilege re-certifications, 2) entity-wide security program issues involving civilian and contractor background investigation weaknesses, 3) inadequately designed and operating change control policies and procedures, and 4) the lack of updated disaster recovery plans which reflect the current environment identified through testing. These weaknesses may increase the risk that the confidentiality, integrity, and availability of system controls and TSA financial data could be exploited thereby compromising the integrity of financial data used by management and reported in TSA's financial statements.

While the recommendations made by KPMG should be considered by TSA, it is the ultimate responsibility of TSA management to determine the most appropriate method(s) for addressing the weaknesses identified based on their system capabilities and available resources.

IT GENERAL CONTROL FINDINGS BY AUDIT AREA

Findings Contributing to a Material Weakness in IT

Conditions: In FY 2008, the following IT and financial system control weaknesses were identified at TSA and contribute to a TSA-level significant deficiency that is considered a material weakness in IT general and application controls.

Application software development and change controls – we noted:

- For the data scripts run at Coast Guard's procedures over approval, testing, and documentation requirements remain in draft form. The does not consistently include all testing, approval, and implementation documentation for all scripts. In addition, Coast Guard does not monitor scripts run in the database through audit logging and has not developed a technical solution to monitor who accesses the database through to run scripts or review what scripts are run.
- An examination of the data scripts run was conducted with an external, independent organization; however, due to the many limitations over scope, the analysis was incomplete. Furthermore, the analysis did not properly evaluate scripts as to financial statement impact, including current versus prior year effect.
- Policies and procedures over software changes for the key financial applications during the development and testing processes include multiple weaknesses over the design as well as the implementation.

Recommendations: Unless specifically noted where TSA needs to take specific corrective action, we recommend that TSA work with the DHS Office of Chief Information Officer (OCIO) to ensure that the Coast Guard complete the following corrective actions:

- Continue to complete and implement the and Change Control Policy.
- Implement and better document a single, integrated script change control process that includes clear lines of authority to Coast Guard financial and IT management personnel, enforced responsibilities of all participants in the process, and documentation requirements.
- Continue efforts to complete an in-depth analysis of active scripts, with the following objectives: All changes to active scripts and new scripts should be subject to an appropriate software change control process to include testing, reviews, and approvals, and all active scripts should be reviewed for impact on financial statement balances.
- Develop and implement change control policies and procedures to verify that all software changes are approved, tested, documented, tracked, and reviewed prior to deploying the changes into the production environment in accordance with DHS Sensitive System Policy Handbook 4300A.

Other Findings in IT General Controls

Although not considered to be a material weakness, we also noted the following other matters related to IT and financial system control deficiencies during the FY08 TSA audit engagement:

1. Access controls – we noted:
   - Access review procedures for key financial applications do not include the review of all user accounts to ensure that all terminated individuals no longer have active accounts, inactive accounts are locked, and privileges associated with each individual are still authorized and necessary.
   - Security configuration management weaknesses exist on hosts supporting the key financial applications and the underlying general support systems.
   - Security patch management weaknesses exist on hosts supporting the key financial applications and general support systems.
   - The computer access agreement and exit clearance procedures for TSA employees have not been consistently implemented.

2. Entity-wide security program planning and management – we noted:
   - The contract between Coast Guard and the support vendor does not include security configuration requirements that must be adhered to during the configuration management process. Coast Guard terminated the contract in FY 2008; however, during the first half of the fiscal year, the contract was still in place and no corrective action had taken place related to the prior year recommendation.
   - Coast Guard's policies and procedures have not been implemented to require that a favorably adjudicated background investigation be completed for all contractor personnel.
   - Background investigations for all civilian Coast Guard employees have not been completed and civilian position sensitivity designations have not been determined in accordance with DHS guidance.
   - There are weaknesses in Specialized Role-based Training for Individuals with Significant Security Responsibilities.
   - A risk assessment for the major financial applications has not been completed and the associated System Security Plan remains in draft form.
   - IT security awareness training has not been completed by all TSA personnel prior to gaining access to the major financial applications.

3. Service continuity – we noted:
   - The Coast Guard Continuity of Operations Plan (COOP) has not been updated to reflect the results of testing and the division Business Continuity Plans have not been finalized. TSA's key financial applications are hosted at

Recommendations: Unless specifically noted where TSA needs to take specific corrective action, we recommend that TSA work with the DHS OCFIO to ensure that the Coast Guard/FINCEN complete the following corrective actions:

1. For access controls:
   - Actively monitor the use of and changes related to operating systems and other sensitive utility software and hardware. Additionally, perform corrective actions on the specific patch and configuration weaknesses identified.
   - Implement the Employee Exit Clearance Procedures by completing, certifying, and maintaining all forms required during the exit process for employees and contractors *(TSA alone needs to take this corrective action)*.
   - Implement the IT Security Policy Handbook by verifying that all TSA employees and contractors sign a computer access agreement prior to being granted system access *(TSA alone needs to take this corrective action)*.
   - Update the quarterly review process to include procedures surrounding the recertification of accounts with elevated privileges on the Unit Approved Plan. In addition, the recertification process should be documented, include supervisor written approval and occur on an at least annual basis *(TSA alone needs to take this corrective action)*.
   - Develop and implement procedures to require a periodic review by supervisors of all financial application and database user accounts and their associated privileges. These procedures should include steps to verify that all terminated individuals no longer have active accounts, that inactive accounts are locked and that privileges associated with each individual are still authorized and necessary.
   - Update procedures to ensure that a documented and approved access authorization request is completed for each individual prior to granting him/her access to the key financial applications or databases.
2. For entity-wide security program planning and management:
   - Create and implement contractor background investigation policies and procedures in order to establish requirements and ensure compliance with DHS Sensitive System Policy Handbook 4300A. This includes the verification that all contracts issued by the Coast Guard include the appropriate Coast Guard position sensitivity designation requirements for contracted personnel.
   - Perform initial background investigations and re-investigations for civilian employees in accordance with position sensitivity designations at no less than the Moderate level as required by DHS directives. In addition, conduct civilian background re-investigations every ten (10) years, as required by DHS directives, to ensure that each employee has a favorably adjudicated and valid Minimum Background Investigation (MBI).
   - Finalize and implement the Role-Based Training which would require personnel with significant information security responsibilities to complete specialized role-based training on an annual basis. Develop and deploy this specialized role-based training and implement the use of the Training Management Tool in order to track and verify specialized role-based training requirements compliance.

- Finalize and implement the C&A Package for the key financial systems in accordance with DHS and National Institute of Standards and Technology (NIST) guidance.
- Enforce mandatory completion of security awareness training by holding groups responsible and accountable as a performance measure for monitoring the training of their employees *(TSA alone needs to take this corrective action).*

3. For service continuity:
   - Update the COOP to include the results of its testing and finalize the applicable supporting business continuity plans.

Cause/Effect: Many of these weaknesses were inherited from the lack of properly designed, detailed, and consistent guidance over financial system controls to enforce DHS Sensitive System Policy Directive 4300A and NIST guidance. The lack of documented and implemented security configuration management controls may result in security responsibilities communicated to system developers improperly as well as the improper implementation and monitoring of system changes by Coast Guard management. This also increases the risk of unsubstantiated changes as well as changes that may introduce errors or data integrity issues that are not easily traceable back to the changes. In addition, it increases the risk of undocumented and unauthorized changes to critical or sensitive information and systems. This may reduce the reliability of information produced by these systems. In addition, reasonable assurance should be provided that financial system user access levels are limited and monitored by both TSA and Coast Guard management for appropriateness and that all user accounts belong to current employees. This is particularly essential for those user accounts that have been identified as having elevated privileges. The weaknesses identified within TSA's access controls increases the risk that employees and contractors may have access to a system that is outside the realm of their job responsibilities or that a separated individual, or another person with knowledge of an active account of a terminated employee, could use the account to alter the data contained within the application or database. This may also increase the risk that the confidentiality, integrity, and availability of system controls and the financial data could be exploited thereby compromising the integrity of financial data used by management and reported in the DHS financial statements. In addition, without proper personnel security measures in place, such as background investigations, TSA financial data could be inappropriately manipulated by contract personnel whose intent is to create havoc or inappropriate financial gain. Lastly, the lack of finalized plans for the recovery of critical operations and key TSA financial system data may potentially increase the risk of delayed recovery efforts during a disaster.

Criteria: The *Federal Information Security Management Act* (FISMA) passed as part of the *Electronic Government Act of 2002,* mandates that Federal entities maintain IT security programs in accordance with OMB and NIST guidance. OMB Circular No. A-130, *Management of Federal Information Resources,* and various NIST guidelines describe specific essential criteria for maintaining effective general IT controls. In addition, OMB Circular No. A-127 prescribes policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. FFMIA sets forth legislation prescribing policies and standards for executive departments and agencies to follow in developing, operating, evaluating, and reporting on financial management systems. The purpose of FFMIA is in relevant part: (1) to provide for consistency of accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government; (2) require Federal financial management systems to support full disclosure of Federal financial data, including the full costs of Federal programs and activities; (3) increase the accountability and credibility of federal financial management; (4)

improve performance, productivity and efficiency of Federal Government financial management; and (5) establish financial management systems to support controlling the cost of Federal Government. In closing, for this year's IT audit we assessed the DHS component's compliance with DHS Sensitive System Policy Directive 4300A.

APPLICATION CONTROL FINDINGS

We did not identify any findings in the area of application controls during the fiscal year 2008 TSA audit engagement.

MANAGEMENT COMMENTS AND OIG RESPONSE

We obtained written comments on a draft of this report from the TSA Assistant Administrator and Chief Financial Officer. Generally, TSA management agreed with all of our findings and recommendations and they have developed a remediation plan to address them. We have incorporated these comments where appropriate and included a copy of the comments in Appendix D.

OIG Response

We agree with the steps that TSA's management is taking to satisfy these recommendations.

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

Appendix A

Description of Key TSA Financial Systems and IT Infrastructure within the Scope of the FY 2008 TSA Financial Statement Audit

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

Below is a description of significant TSA financial management systems and supporting Information Technology (IT) infrastructure included in the scope of the engagement to perform the financial statement audit.

Locations of Audit: TSA in and the Coast Guard . TSA's financial applications are hosted on the Coast Guard's IT platforms.

Key Systems Subject to Audit:

- : Core accounting system that is the principal general ledger for recording financial transactions for the Coast Guard. is hosted at , the Coast Guard's primary data center. It is a customized version of Financials.
- : Used to create and post obligations to the core accounting system. It allows users to enter funding, create purchase requests, issue procurement documents, perform system administration responsibilities, and reconcile weekly program element status reports. is interconnected with the system and is hosted at .
- *:* is a customized third party commercial off the shelf (COTS) product hosted at and used for TSA and property management. interacts directly with the module in Additionally, is interconnected to the system.

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

Appendix B

FY2008 Notice of IT Findings and Recommendations – Transportation Security Administration

Notice of Findings and Recommendations – Definition of Risk Ratings:**

The Notices of Findings and Recommendations (NFR) were risk ranked as High, Medium, and Low** based upon the potential impact that each weakness could have on TSA's information technology (IT) general control environment and the integrity of the financial data residing on TSA's financial systems, and the pervasiveness of the weakness.

** **The risk ratings are intended only to assist management in prioritizing corrective actions**, considering the potential benefit of the corrective action to strengthen the IT general control environment and/or the integrity of the DHS consolidated financial statements. The risk ratings, used in this context, are not defined by *Government Auditing Standards*, issued by the Comptroller General of the United States, or the American Institute of Certified Public Accountants (AICPA) Professional Standards, and do not necessarily correlate to a significant deficiency, as defined by the AICPA Standards and reported in our *Independent Auditors' Report* on the TSA balance sheet, dated March 6, 2009.

Correction of some higher risk findings may help mitigate the severity of lower risk findings, and possibly function as a compensating control. In addition, analysis was conducted collectively on all NFRs to assess connections between individual NFRs, which when joined together could lead to a control weakness occurring with more likelihood and/or higher impact potential.

High Risk**: A control weakness that is more serious in nature affecting a broader range of financial IT systems, or having a more significant impact on the IT general control environment and /or the integrity of the financial statements as a whole.

Medium Risk**: A control weakness that is less severe in nature, but in conjunction with other IT general control weaknesses identified, may have a significant impact on the IT general control environment and / or the integrity of the financial statements as a whole.

Low Risk**: A control weakness minimal in impact to the IT general control environment and / or the integrity of the financial statements.

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

Transportation Security Administration
FY2008 Information Technology - Notice of Findings and Recommendations – Detail

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

Department of Homeland Security
Transportation Security Administration
FY2008 Information Technology
Notice of Findings and Recommendations – Detail

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
IT-08-01	The COOP has not been updated to reflect the results of testing and the division business continuity plans have not been finalized.	We recommend that TSA monitor efforts to update the COOP as the result of its testing and finalize the applicable supporting business continuity plans.		X	Low
IT-08-03	During the first half of the year, the contract with the , and software vendor was still in place and no corrective action taken had taken place related to the prior year recommendation. Therefore, the risk of the preexisting condition was present for the majority of the year (October 1, 2007 through April 1, 2008). However due to the Coast Guard decision to terminate the contract with their software vendor, and the Coast Guard Headquarters decision to suspend all SPRs and SCRs until the instructions are lifted this condition did not exist beyond the date of these two events.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters completes, in a timely manner, the planned corrective actions of the following: • Coast Guard Headquarters enhance their existing Configuration Management/Change Management policies and procedures to explicitly address security configurations and software patches (e.g., those associated with system/application "builds", service packs, and maintenance releases) to better ensure compliance with DHS requirements and NIST guidance. • Coast Guard Headquarters and the applicable Coast Guard locations communicate with and educate affected staff regarding these improved policies and procedures. • Coast Guard Headquarters develop, communicate, and implement procedures to periodically review system changes and system baselines.		X	High

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
IT-08-05	Coast Guard Headquarters has developed but not yet implemented policies or procedures to require that a favorably adjudicated background investigation be completed for all contractor personnel.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters completes, in a timely manner, the planned corrective actions to create and implement contractor background investigation policies and procedures in order to establish requirements and ensure compliance with DHS Sensitive System Policy Directive 4300A. This includes the verification that all contracts issued by the Coast Guard include the appropriate Coast Guard position sensitivity designation requirements for contracted personnel.		X	High
IT-08-06	The Role-Based Training for USCG Information Assurance Professionals Commandant Instruction is still in draft form and has not been fully implemented.	We recommend that TSA monitor Coast Guard Headquarters' efforts to complete planned corrective actions to: • Continue efforts to finalize and implement the Role-Based Training for USCG Information Assurance Professionals Commandant Instruction which would require personnel with significant information security responsibilities to complete specialized role-based training on an annual basis. • Develop and deploy this specialized role-based training throughout the Coast Guard. • Implement the use of the Training Management Tool in order to track and verify specialized role-based training requirements compliance.		X	Medium

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
IT-08-13	FINCEN is in the process of updating and finalizing the C&A Package for the . The comprehensive CAS Suite SSP will include the major subsystems , and and financial supporting applications and will be used instead of an individual SSP for each system. The also identifies the management controls around risk assessments, planning, security assessments, , and systems and services acquisition.	We recommend that TSA monitor that is taking corrective action to finalize and implement the C&A Package for the in accordance with DHS and NIST guidance.		X	Low
IT-08-15	Of the 669 employees/contractors with current access to the following TSA's financial applications: , ; 152 employees/contractors have not completed the IT Security Awareness Training.	We recommend that TSA perform the following corrective actions: • Enforce mandatory completion of Security Awareness Training by holding groups responsible and accountable as a performance measure for monitoring the training of their employees. • Revoke system access of employees who do not complete the required annual security awareness training before the deadline and until the employees subsequently completes the required training.		X	Medium
IT-08-18	Configuration management weaknesses continue to exist on hosts supporting the and applications and the . Note: See the tables in the NFR for the specific conditions.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard's completes, in a timely manner, the planned corrective actions of the following: • Implement the corrective actions noted in the tables above. • Implement polices and procedures to ensure that the software builds created by CG are tested, prior to implementation, to ensure that all software security configurations, such as software patches and non-compliant settings, are up to date.		X	Medium

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
IT-08-19	Patch management weaknesses continue to exist on hosts supporting the and applications and the . Note: See the tables in the NFR for the specific conditions.	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the planned corrective actions of the following: • Implement the corrective actions noted in the NFR. • Implement polices and procedures to ensure that the software builds created by CG are tested, prior to implementation, to ensure that all software security configurations, such as software patches.		X	Medium
IT-08-20	We were unable to obtain 21 1163 Forms and 27 1402 Forms for each sample of 40. Additionally, 2 of the 13 1402 Forms received were signed after the forms were requested for audit. The IT Security Policy Handbook requires all TSA personnel including contractors to review and sign the TSA Form 1403: Computer Access Agreement. However, we were unable to obtain 7 of the 25, 1403: *Computer Access Agreements* sampled. Of the 18 forms we obtained, 5 were dated after the sample was requested for audit.	We recommend that TSA perform the following corrective actions: • Implement the Employee Exit Clearance Procedures by completing, certifying, and maintaining all forms required during the exit process for employees and contractors. • Implement the IT Security Policy Handbook by verifying that all TSA employees and contractors sign a computer access agreement prior to being granted system access.		X	Medium
IT-08-21	The change control policy has not been fully completed and implemented. The United States Coast Guard (CG) is responsible for making software changes to the and applications, however, on March 31, 2008, CG HQ terminated its contract with the software vendor/developer for , and , which has hindered TSA's ability to fully complete and implement the and change control policy.	We recommend TSA continue to complete and implements the following sections of the , Change Control Policy: Build Selection Process, Software Development Process, and Software Testing Process.		X	Medium
IT-08-22	Control weaknesses still exist within the design of	We recommend that TSA work with the DHS		X	High

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	Coast Guard's Configuration Management policies and procedures for , as well as the operating effectiveness of those controls. Our test work over the design of the change controls covered both periods of the change control environment; however, our testing of operating effectiveness covered only the period of start of the fiscal year through March 2008, since there were no changes made to from April through the remainder of the fiscal year.	Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the planned corrective actions of the following: • The develop, implement, communicate, and enforce procedures regarding how changes are to be controlled, documented, tracked, and reviewed as these changes progress through testing and into production. • Coast Guard Headquarters develop, implement, communicate, and enforce procedures regarding how change control documentation will be maintained, reviewed, and validated in accordance with DHS Sensitive System Policy Directive 4300A.			
IT-08-23	Coast Guard's controls over the scripting process remain ineffective. Weaknesses were noted in controls over script implementation, approvals and testing, as well as active script modification. In addition, Coast Guard has not maintained or developed a population of scripts run since the inception of in 2003 nor has it performed a historical analysis of script impact on the cumulative balances in permanent accounts of the financial statements. Specifically: • Coast Guard lacks a formal process to distinguish between the module lead approvers for script approval requests (Conditions #1 & #2); • The Procedures for Data Scripts do not specifically state the testing and documentation requirements for blanket approval scripts and this policy remains in draft form (Conditions # 3 & #4); • Coast Guard does not monitor scripts run in the	TSA does not have the ability to take corrective actions to remediate these control issues on their own. Therefore it should be made clear that TSA is dependent on the Coast Guard to take the necessary action. In order for management to assert to any financial statement line items, we recommend that TSA work with the DHS Chief Financial Officer and the DHS Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the planned corrective actions to: • Continue to design, document, implement, and demonstrate the effectiveness of internal controls associated with the active (current and future) scripts. • Identify and evaluate the historical scripts (all those implemented prior to those identified in recommendation 1 above) to determine the financial statement impact on cumulative		X	High

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
	database through audit logging and has not developed a technical solution to monitor who accesses the database through to run scripts or review what scripts are run (Conditions #5 & #6); • The does not consistently include all testing, approval, and implementation documentation for all scripts (Condition #7); and • Coast Guard has not completed documentation for all scripts executed since their implementation (Condition #8). Additionally, although Coast Guard did conduct an examination with an external contractor organization, we have determined that the analysis was incomplete. Specifically, due to the many limitations over scope, it did not consider the full population of scripts run at currently or since the inception of . Furthermore, the analysis did not properly evaluate scripts as to financial statement impact, including current versus prior year effect (Condition #9)	balances in permanent accounts; and develop and maintain supporting procedures related to each script. With respect to procedures already in place, TSA should work with the DHS Chief Financial Officer and the DHS Chief Information Officer to ensure that Coast Guard Headquarters completes, in a timely manner, the corrective actions to: • Continue to update script policies and procedures to include clear guidance over module lead approvers, testing and documentation requirements, monitoring/audit log reviews, and blanket approval requirements. • Finalize and implement policies and procedures governing the script change control process including completing records within the for all executed scripts and ensuring that all scripts are tested in an appropriate test environment prior to being put into production. Regarding the actual scripts themselves, TSA should work with the DHS Chief Financial Officer and the DHS Chief Information Officer to ensure that Coast Guard Headquarters completes, in a timely manner, the corrective actions to: • Determine the root causes and specific detailed actions necessary to correct the conditions that resulted in scripts, for the total population of scripts run at in order to develop system upgrades that would eliminate the use of some of the scripts. • Continue efforts to complete an in-depth analysis of active scripts, with the following			

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
		objectives: o All changes to active scripts and new scripts should be subject to an appropriate software change control process to include testing, reviews, and approvals. o All active scripts should be reviewed for impact on financial statement balances.			
IT-08-24	Although Coast Guard Headquarters is in the process of completing background investigations for all civilian employees, this has not been completed. Additionally, Coast Guard has set its position sensitivity designations to Low for the majority of its employees. However, DHS requires position sensitivity designations no less than Moderate which equates to a Minimum Background Check (MBI).	We recommend that TSA work with the DHS Chief Information Officer to ensure that Coast Guard Headquarters' completes, in a timely manner, the following planned corrective actions: • Perform the initial background investigations and re-investigations for civilian employees in accordance with position sensitivity designations at no less than the Moderate level as required by DHS directives; and • Conduct civilian background re-investigations every ten (10) years, as required by DHS directives, to ensure that each employee has a favorably adjudicated and valid MBI		X	Medium
IT-08-26	Although procedures surrounding user access privilege re-certifications have been developed, we noted that the process does not include all , and users and does not involve users' supervisors as required by DHS Sensitive System Policy Directive 4300A. Additionally, we noted that AAR forms are not being completed for all users on a consistent basis and we identified instances where system access was granted prior to the AAR approval by a supervisor.	We recommend that TSA work with the DHS Chief Information Officer to ensure that the Coast Guard's completes, in a timely manner, the planned corrective actions to: • Implement and document the user access review procedures to include all access privileges and include supervisors in each review. • Update procedures to ensure that a documented and approved access authorization request is completed for each individual prior to granting him/her access to the and applications or	X		Medium

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

NFR #	Condition	Recommendation	New Issue	Repeat Issue	Risk Rating*
		databases.			
IT-08-27	Although TSA has implemented quarterly access reviews for user accounts and identified accounts with elevated privileges, TSA has not ensured that the accounts with an increased risk associated with them are reviewed/authorized on a periodic basis by a supervisor.	We recommend that TSA update the and Site Administrator User and Role Quarterly Review Process to include procedures surrounding the recertification of accounts with elevated privileges on the Unit Approved Plan. In addition, the recertification process should be documented, include supervisor written approval and occur on an at least annual basis.	X		Medium

*** Risk ratings are only intended to assist management in prioritizing corrective actions. Risk ratings in this context do not correlate to definitions of control deficiencies as identified by the AICPA.**

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

Appendix C

Status of Prior Year Notices of Findings and Recommendations And Comparison To Current Year Notices of Findings and Recommendations

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

Current Year Notices of Findings and Recommendations at TSA

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA- IT-07-01	The disaster recovery aspect of the COOP will be completed by September 30, 2007 with the business continuity and continuity of government aspects of the COOP not being completed until December 2007. Because the COOP is in draft form, it has not yet been tested; however, plans to test the entire COOP prior to it being implemented. Lastly, the has drafted a memorandum of understanding (MOU) with the for reciprocal services; however, the MOU is currently in draft form.		08-01
TSA- IT-07-02	is in the process of developing of a Continuity of Operations Plan (COOP) which addresses disaster recovery, business continuity and continuity of government for . The disaster recovery aspect of the COOP will be completed by September 30, 2007 with the business continuity and continuity of government aspects of the COOP not being completed until December 2007. Because the COOP is in draft form, it has not yet been tested; however, plans to test the entire COOP prior to it being implemented. Lastly, the has drafted a MOU with the for reciprocal services; however, the MOU is currently in draft form.	X	
TSA-IT-07-03	The contract that CG HQ has with the and software vendor does not include security configuration requirements that must be adhered to during the configuration management process. Consequently, and builds and maintenance packs may not be configured and implemented with comprehensive security configuration requirements. CG recognizes the absence of security requirements and indicated that the contract with the vendor will be reassessed in 2008 during the contract renewal process with CG HQ and corrective actions will be taken at that time.		08-03
TSA-IT-07-04	19 individuals, specified below, had 24 hour a day access to the data center and had not yet completed the training: - 13 individuals (building owners, property managers and their respective contractors); - 4 members of Senior Management; and - 2 security guards. Lastly, we identified four employees, each with 24 hour access to the data center that had not yet completed the training as of July 2007. Upon notifying of this exception, the four individuals completed the training and provided KPMG with supporting evidence.	X	

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA-IT-07-05	No formal procedures have been developed or implemented by Coast Guard Headquarters to address DHS requirements surrounding the suitability screening of contractors accessing DHS IT systems. DHS directives and policies require Coast Guard and other DHS components to ensure the completion of background investigations for all contractors accessing IT systems. The type of background investigations should be based on the risk level of their future position at CG and are required to be completed prior to the start of work. However, no CG guidance exists to require CG components to clear their contractors for suitability, especially those with sensitive IT positions.		08-05
TSA-IT-07-06	The IT Security Awareness, Training and Education Plan lacks appropriate criteria for defining personnel with significant IT responsibilities. Additionally, the personnel that are defined in the guidance are very limited and do not fully cover the scope of security responsibilities addressed in DHS requirements.		08-06
TSA-IT-07-07	• TSA management did not receive a response from the Federal Air Marshalls Service Division user base for the May and for the July 2007 review. Therefore, TSA assumed that no response indicated that all roles were appropriate and did not follow-up to ensure that a response was received. • Privileges associated with each user were not included in the May and July 2007 reviews performed. We also noted that the accounts of terminated employees are not removed from the system in a timely manner. Although TSA requested that several of the accounts of terminated individuals be deactivated/end-dated by , the requests were not submitted to FINCEN until months after the employees departed and we were unable to obtain evidence that these accounts had in fact been deactivated/end-dated.	X	
TSA-IT-07-08	• The application and database does not meet the password requirements noted in DHS Sensitive System Policy Directive 4300A. • accounts of terminated individuals are not removed in a timely manner including one individual who had user account management capabilities within the system. • application and database accounts are not being reviewed for appropriateness.	X	

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA-IT-07-09	• We were unable to obtain a copy of the password configuration. However, we performed a demonstration/walkthrough of the password with a point of contact and were able to determine that the password configuration is not in compliance with DHS guidance. • Although the system has been configured to track and lock accounts that have not been utilized in 90 days, DHS guidance requires that accounts that have not been used in 30 days be deactivated.	X	
TSA-IT-07-10	An excessive number of individuals had user administration capabilities within FPD until the implementation of the centralized user management (August 19, 2007). We also noted the existence of two shared generic accounts with this privilege: and . These accounts have every privilege within the application, including the ability to create/delete/modify user accounts within .	X	
TSA-IT-07-11	• Accounts of terminated employees and contractors are not removed from the system in a timely manner. Specifically, accounts of terminated employees and contractors have not been end-dated and accounts of terminated employees and contractors were not end-dated until months after their departure. • periodic account reviews are not being performed to ensure that all users are current employees or contractors and that their privileges are still required to perform their job functions. • Three of 15 Financial Systems Access Request Forms were not completed in their entirety. Specifically, the three forms did not contain the privileges that each user was to be granted within the system.	X	
TSA-IT-07-12	The accounts of terminated contractors are not end-dated or disabled in a timely manner. Additionally, we noted that TSA has not developed policies or procedures that require a periodic review of application and database accounts, and their associated privileges, be performed to determine that access is appropriate.	X	
TSA-IT-07-13	Management had not adequately completed the Certification and Accreditation (C&A) package to include the system. Specifically, management stated that Sunflower is a subsystem of and a separate C&A does not need to be completed since it is covered by the C&A Package. However, we determined that there is no documentation within the System Security Plan that defines as a subsystem and specifically addresses the appropriate security controls for in this capacity.		08-13
TSA-IT-07-14	systems have been configured to automatically end date accounts that have not been used in six months; however, DHS guidance requires accounts that have been inactive for 30 days be disabled.	X	

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA-IT-07-15	The policies and procedures over a formalized sanctioning process have not been fully developed and implemented. Specifically, the policies and procedures do not include consequences for individuals who do not sign the computer access agreements or complete initial or refresher security awareness training. Furthermore, out of the nine individuals selected, only one had completed a Computer Access Agreement. Additionally, we determined that TSA allows individuals to complete security awareness training within sixty days of beginning work and gaining access to their and application accounts. However DHS guidance requires that all individuals complete security awareness training prior to gaining access to the Information systems. Furthermore, out of the selection of nine individuals, one contractor had not completed initial security awareness training this fiscal year and a second employee had not completed their refresher training for this fiscal year.		08-15
TSA-IT-07-16	Procedures are not formally documented requiring the review of the activities of the system administrators. We also noted that reviews of the audit logs that document the actions of administrators in the operating environment are not being performed.	X	
TSA-IT-07-17	Procedures are not formally documented identifying how change control should be performed when applying system software changes, including software patches, to the operating system according to a standard schedule or in an emergency situation. While a policy exists, it lacks detailed procedures in order to be effective.	X	
TSA-IT-07-18	Configuration management weaknesses continue to exist on hosts supporting the and applications and the . Note: See the tables in the NFR for the specific conditions.		08-18
TSA-IT-07-19	Patch management weaknesses continue to exist on hosts supporting the and applications and the . Note: See the tables in the NFR for the specific conditions.		08-19

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA-IT-07-20	Implementation of the formalized exit process for TSA personnel policies and procedures has not been fully executed. Specifically, only eleven (11) out of a selection of thirty (30) TSA 1402 Forms, the Separating Non-Screener Employee and Contractor IT Certificates, were received. Additionally, of the eleven received, seven (7) of the forms did not have the appropriate TSA application(s) identified in order to deactivate the separating employee's accounts. Furthermore, we selected thirty (30) TSA 1163 forms, the Employee Exit Clearance form, for both contractors and TSA personnel and only received nine (9) completed forms. The purpose of the 1163 form is to document sign-offs for access removal of financial and related administrative system accounts for applications such as access to the Intranet.		08-20
TSA-IT-07-21	1. TSA has not fully documented policies and procedures surrounding the change control process for to define the overlap in the responsibilities between TSA and or guidance for ensuring that changes that are passed/deferred to are tested and operate appropriately prior to approval by TSA and implementation into production. 2. Additionally, TSA does not consistently retain documentation associated with the changes. 3. Policies and procedures for the emergency change control process are not documented.		08-21
TSA-IT-07-22	has not fully developed and implemented their policies and procedures for the change control and emergency change control process to guide staff in the implementation of this process at . Specifically, we noted that the policies and procedures remain at a high-level and to do not include requirements for who is responsible for the initial approvals of the changes proposed by the vendor, including technical changes, the testing plan requirements for each phase of testing and the capacity in which is involved, and the final approval of all changes to the system. Instead, the procedures detail the overall process and phases for and change control, but lack detailed guidance for the roles and responsibilities executed by personnel. Additionally, we noted that follows the same change control process for emergency changes. However, the details surrounding that emergency change control process are not formally documented in the procedures for and . For example, requirements for the categorization of priority levels and response time requirements for each priority level are not included.		08-22

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
	Furthermore, has not fully implemented the procedures documented in the System Change Procedures. Specifically, we noted that were not completed for changes made to the suite as of June 2006. Upon review of a selection of changes, we determined that is not consistently retaining documentation to support the change control and emergency change control process. Specifically, we inspected documentation associated with 30 and system changes and emergency changes and determined that various pieces of supporting documentation (i.e., functional resolution documents, test plans for the different phases of testing, evidence of testing, and approvals) were insufficient and/or not available for all 30 of the changes and emergency changes selected for testing.		
TSA-IT-07-23	Coast Guard change controls related to Coast Guard and TSA financial systems are not appropriately designed, operating effectively or in compliance with Office of Management and Budget Circular No. A-130, Security of Federal Automated Information Resources, the DHS Sensitive System Policy Directive 4300A and the National Institute of Standards and Technology Special Publications. Coast Guard has and continues to operate a separate, informal and largely undocumented change development and implementation process effecting Coast Guard and TSA Financial Systems, outside of and conflicting with the formal change control process. Coast Guard is unable to provide a complete population of implemented scripts, to include the type, purpose and intended effect on both CG and TSA financial data. The implemented process is ineffective as the approval, testing and documentation procedures of the script changes are not appropriately designed and the current process is ineffective to control the intended and actual effect on TSA financial data. Coast Guard has only eliminated a small number of the scripts used on a consistent basis and is projecting that this approach will continue into the delivery of and beyond.		08-23
TSA-IT-07-24	Civilian background investigations and reinvestigations are not being performed in accordance with DHS guidance. Specifically, sixteen (16) out of twenty (20) individual background investigations reviewed did not meet the DHS minimum standard of investigation of an MBI per DHS Sensitive System Policy Directive 4300A. Furthermore, upon review of a selection of five (5) civilian personnel, one (1) individual had an investigation that had not been adjudicated since 1988. DHS guidance requires that civilian personnel are reinvestigated every ten (10) years.		08-24

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

		Disposition	
NFR No.	**Description**	**Closed**	**Repeat**
TSA-IT-07-25	TSA has not taken corrective actions to develop and implement TSA specific change control policies and procedures for the TSA change control or emergency change control process. Furthermore, upon review of a selection of changes, we determined that TSA is not consistently implementing the change control process. Specifically, we inspected documentation associated with seven system changes and emergency changes and determined that supporting documentation (i.e., test plans, evidence of testing, and approvals to move the change into production) were not available for all seven of the changes and emergency changes selected for testing. Additionally, KPMG noted that testing was not fully completed by TSA prior to passing the change for testing for three of the changes.	X	

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

Appendix D

Management Comments

Department of Homeland Security
Transportation Security Administration
Information Technology Management Letter
September 30, 2008

U.S. Department of Homeland Security

Office of Finance and Administration
601 South 12th Street, TSA-14
Arlington, VA 20598-6014

Transportation Security Administration

FEB 27 2009

Mr. Frank Deffer
Assistant Inspector General, Information Technology Audits
Department of Homeland Security
Washington, DC 20528

Dear Mr. Deffer:

Thank you for the opportunity to comment on the draft audit report "*Information Technology Management Letter for the FY 2008 Transportation Security Administration (TSA) Financial Statement Audit*". While we concur with all of the recommendations, we would like to point out that a majority of findings noted in the report, and all of the findings which contribute to the material weakness, stem from TSA's use of the U.S. Coast Guard (USCG) Financial Systems and the services provided by USCG's Finance Center. As such, TSA's ability to take unilateral action to correct the conditions noted in the report is inherently limited.

Despite the limitations of our cross-serviced financial systems environment, TSA and USCG made significant progress to address audit findings in FY 2008. As the report noted, 12 of the 25 audit findings reported in FY 2007 were remediated in FY 2008, while only two new medium-risk findings were identified. This nearly 50% reduction in weaknesses was the result of collaborative efforts between TSA financial management and information technology personnel and their USCG counterparts. In FY 2009, TSA will continue to work closely with USCG and the Department of Homeland Security (DHS) Chief Information Officer to implement new processes, procedures, and controls to strengthen our financial management systems, address the audit findings, and lead to remediation of the material weakness.

As required by the DHS Chief Financial Officer, TSA has prepared a series of comprehensive Mission Action Plans (MAPs). The MAPs outline required corrective actions necessary to remediate weaknesses identified by your audit and provide milestone completion dates for those actions. TSA briefed its FY 2009 MAPs to DHS on January 29, 2009, and will conduct monthly MAP progress briefings beginning in March 2009. DHS Inspector General personnel are invited to attend these briefings.

File 1000.1

www.tsa.gov

In closing, we appreciate the recommendations and insight offered in your audit and look forward to working with your team during the upcoming FY 2009 financial audit.

Sincerely,

Maureen L. Smith, Acting

David R. Nicholson
Assistant Administrator and Chief Financial Officer
Office of Finance and Administration

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Policy
Chief of Staff for Operations
Acting General Counsel
Executive Secretariat
Under Secretary, Management
Acting Assistant Commissioner, TSA
DHS Chief Information Officer
DHS Chief Financial Officer
Chief Financial Officer, TSA
Acting Chief Information Officer, TSA
Chief Information Security Officer
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS GAO OIG Audit Liaison
Chief Information Officer, Audit Liaison
TSA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees as Appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.